ПРО ПІДВИЩЕННЯ БЕЗПЕКИ ОБМІНУ ФАЙЛАМИ У ВІДЕОКОНФЕРЕНЦІЯХ

Філімонов Д.А., д.т.н., проф. Антіпов І.Є.
Харківський національний університет радіоелектроніки,
кафедра КРіСТЗІ, м. Харків, Україна
e-mail: denis.filimonov@nure.ua

Abstract. Theses are about the files protecting that are transferred within the videoconference. Onion nesting and file encryption are suggested. According to algorithm, one of the layers contains a mechanism for comparison the real and expected IP-address. In case of a match, the inner protective layer is removed and the file becomes available. If there is a mismatch, the data will be destroyed. The algorithm will make it impossible to intercept attached files from a media stream that is weakly protected.

Актуальність відеоконференцій (ВК) є незаперечною. В наш час вони використовуються повсюдно від навчання та проведення судових засідань до міждержавних переговорів на найвищому рівні. ВК реалізуються через комп'ютер, планшет чи телефон і можуть супроводжуватися додатковим показом презентації, демонстрацією екрану та ін. Ряд сервісів дозволяють також обмінюватися файлами.

У доповіді запропоновано спосіб підвищення безпеки обміну файлами, що передаються у рамках ВК. Для його реалізації необхідно знати IP-адресу одержувачів – учасників даної ВК, які з'ясовуються на етапі їхньої авторизації при підключенні до відповідного сервісу.

Алгоритм формування даних, що передаються, наступний. Перед передачею файлу, він попередньо зашифровується за допомогою алгоритму AES. Потім відбувається інтеграція очікуваних IP-адрес одержувачів і механізму їх перевірки в передані дані, які ще раз зашифровуються AES. В результаті формується масив, схематично показаний на рис. 1. Після чого він передається по мережі разом із медіапотоком.

Механізм перевірки, що входить до складу масиву, являє собою програмний код, який вбудований таким чином, що після шифрування разом з IP-адресами утворює з ними єдине ціле. Цей масив може бути модифікований без порушення працездатності механізму перевірки. Рисунок 1

У постійному вигляді вказаний масив проходить по мережі до адресата. При отриманні файлу миттєво та автоматично запускається первинний механізм дешифрування, який перевіряє IP-адреси на відповідність до очікуваних. У разі збігу очікуваної та реальної IP-адреси відбувається зняття «внутрішнього» шару шифрування та вилучення вихідного файлу, що схематично представлено на рис. 2. Усі процедури відбуваються у клієнтській частині додатку для ВК.

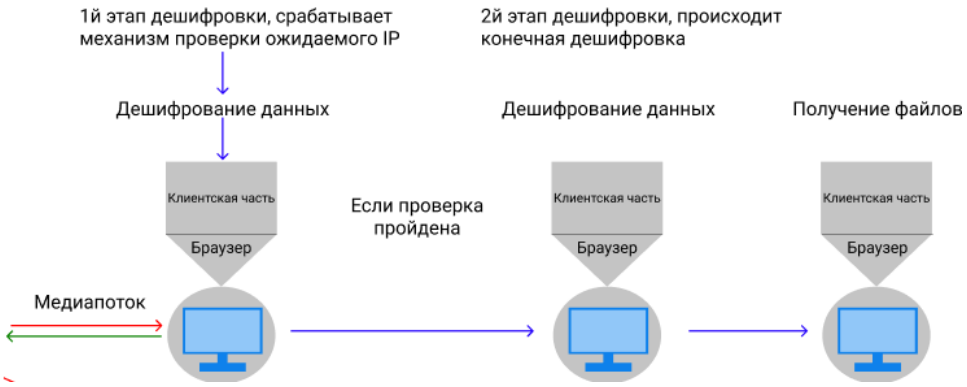

Рисунок 2

Особливостями WEB-протоколів, що використовуються при організації ВК, є те, що, по-перше, «недоставка» даних не впливає на продовження трансляції, а по-друге, не існує механізму перевірки адрес усіх одержувачів медіапотоку. Це дозволяє зловмиснику перехоплювати дані, залишаючись при цьому непомітним.

Але при отриманні зловмисником файлу, зашифрованого пропонованим способом, після запуску механізму дешифрування виявляється розбіжність реальної IP-адреси і тієї, яка закладена в механізм перевірки. І тут зняття «внутрішнього» шару шифрування немає, а отриманий масив даних знищується, що схематично представлено на рис. 3.

Оскільки всі процедури відбуваються в клієнтській частині спеціальної програми, то зловмисник не має змоги отримати доступ до даних після зняття «зовнішнього» шару шифрування.

Хоча даний алгоритм розроблений саме для файлів, що передаються в рамках ВК, при певному доопрацюванні він може бути застосований і для медіапотоку.

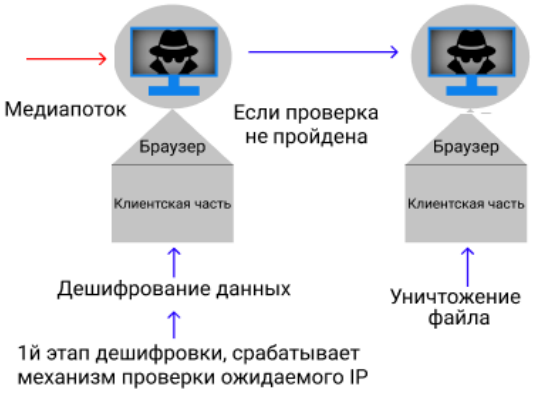

Рисунок 3